REMOTE AUTHENTICATION BASED ON EXCHANGING
SIGNALS REPRESENTING BIOMETRICS INFORMATION

5   **ABSTRACT**

A method, an apparatus, and a computer program product for remote authentication
are disclosed. The methods are based on exchanging of signals representing remote
party's biometrics information (such as acoustic waveforms) and have application in
secure telephony or video-conferencing communications over open networks. The

10   apparatus includes a speech encoding/decoding module (632), a control module (636),
an encryption/decryption module (640), a key generator (650), a Diffie Hellman key
exchange system (660), a timer module (670) for measuring time between a
challenged statement and a corresponding response statement, an input/output (I/O)
module (680) for transmitting and receiving data via a communications channel 610.

15   FIG. 6